Notice of Allowability	Application No.	Applicant(s)	
	09/719,193	GOUBIN ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Terminal Disclaimer to obviate a double patenting rejection filed on 12/7/2005*.

2. ☒ The allowed claim(s) is/are *27-47*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☒ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☒ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Terminal Disclaimer

The terminal disclaimer filed on 12/7/2005 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 6,658,569 has been reviewed and is accepted. The terminal disclaimer has been recorded.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Page 1, line 31 of the Specification **filed on 12/8/2000** contains a URL which is used in order to incorporate the document entitled "Introduction to Differential Power Analysis and Related Attacks" (Kocher et al.) into the present application by reference. This is not permitted according to 37 CFR 1.57(d).

Please Amend the Application as follows:

On page 1 **delete** line 30 containing

"found at the URL address:"

On page 1 **delete** line 31 containing

"http://www.cryptography.com/dpa/technical/index.html"

Allowable Subject Matter

Claims 27-47 are allowed.

The following is an examiner's statement of reasons for allowance: The above mentioned claims are allowable over the prior arts because the CPA (Cited Prior Arts) of record taken singly or in combination fail to anticipate or render obvious the specific added limitations, as recited in independent claims 27 and 33 and subsequent dependent claims.

The CPA does not teach or suggest a system and method of separating a standard cryptographic algorithm into a plurality of simultaneous calculation processes **based on** the secret data (Ds). Furthermore, the CPA does not teach or suggest a system or method of reconstituting a final result, corresponding to a result of the standard cryptographic algorithm from the plurality of partial results which were created by applying nonlinear transformations to, specifically, each of the partial intermediate variables.

The present invention addresses the following drawbacks of the prior art: The algorithm is calculated based on the data, thereby making it less vulnerable to attacks and more specifically less vulnerable to a Differential Key Differential Power Analysis (DKDPA).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 4,993,068
2. US Patent No. 5,588,059
3. US Patent No. 5,850,443
4. Kocher et al., "Introduction to Differential Power Analysis and Related Attacks"

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2137
12/23/2005

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER